DOCKET NO.: 5895P044

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

JAE DOO HUH, ET AL.

Application No.:

Filed:

For: **KEY MANAGEMENT DEVICE AND METHOD FOR PROVIDING SECURITY SERVICE IN ETHERNET-BASED PASSIVE OPTICAL NETWORK**

Art Group:

Examiner:

Commissioner for Patents
P.O, Box 1450
Alexandria, VA 22313-1450

REQUEST FOR PRIORITY

Sir:

Applicant respectfully requests a convention priority for the above-captioned application, namely:

COUNTRY	APPLICATION NUMBER	DATE OF FILING
Korea	10-2003-0046490	9 July 2003

☒ A certified copy of the document is being submitted herewith.

Respectfully submitted,

Blakely, Sokoloff, Taylor & Zafman LLP

Dated: 10/7/03

Eric S. Hyman, Reg. No. 30,139

12400 Wilshire Blvd., 7th Floor
Los Angeles, California 90025
Telephone: (310) 207-3800

대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0046490
Application Number

출 원 년 월 일 : 2003년 07월 09일
Date of Application JUL 09, 2003

출 원 인 : 한국전자통신연구원
Applicant(s) Electronics and Telecommunications Research Insi

2003 년 10 월 07 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0001
【제출일자】	2003.07.09
【발명의 명칭】	이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 장치 및 방법
【발명의 영문명칭】	KEY MANAGEMENT DEVICE AND METHOD FOR PROVIDING SECURITY SERVICE IN EPON
【출원인】	
【명칭】	한국전자통신연구원
【출원인코드】	3-1998-007763-8
【대리인】	
【명칭】	특허법인씨엔에스
【대리인코드】	9-2003-100065-1
【지정된변리사】	손원 ,함상준
【포괄위임등록번호】	2003-046223-6
【발명자】	
【성명의 국문표기】	허재두
【성명의 영문표기】	HUH,Jae Doo
【주민등록번호】	610816-1696611
【우편번호】	302-753
【주소】	대전광역시 서구 월평동 한아름아파트 101-1205
【국적】	KR
【발명자】	
【성명의 국문표기】	최수일
【성명의 영문표기】	CHOI,Su Il
【주민등록번호】	671220-1551717
【우편번호】	302-759
【주소】	대전광역시 서구 월평2동 샛별아파트 103동 509호
【국적】	KR

【발명자】

【성명의 국문표기】 안경환
【성명의 영문표기】 AHN,Kyeong Whan
【주민등록번호】 711228-1787510
【우편번호】 702-010
【주소】 대구광역시 북구 산격동 1370
【국적】 KR

【발명자】

【성명의 국문표기】 한기준
【성명의 영문표기】 HAN,Ki Jun
【주민등록번호】 550823-1066631
【우편번호】 706-766
【주소】 대구광역시 수성구 범물동 서한아파트 103-501
【국적】 KR

【공지예외적용대상증명서류의 내용】

【공개형태】 간행물 발표 '2003년 정보 네트워킹 국제 회의'
【공개일자】 2003.02.12

【심사청구】 청구

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인
특허법인씨엔에스 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	21	면	21,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	35	항	1,229,000 원

【합계】 1,279,000 원
【감면사유】 정부출연연구기관
【감면후 수수료】 639,500 원

【기술이전】

【기술양도】 희망
【실시권 허여】 희망
【기술지도】 희망

【첨부서류】 1. 요약서·명세서(도면)_1통 2.공지예외적용대상(신규성상실의예외, 출원시의특례)규정을 적용받 기 위한 증명서류_1통 3.정부출연연구기관등의 설립운영및육성에관한법률 제2조에의한 정부 출연연구기관에 해당함을 증명하는 서류_1통

【요약서】

【요약】

본 발명은 이더넷 기반 수동형 광네트워크(EPON)에 관한 것으로서, 특히 이더넷 특성상 보안에 취약한 EPON에서 보안 서비스를 제공하기 위해 요구되는 키관리 장치 및 방법에 관한 것이다. 본 발명은 광종단장치(OLT)와 광가입자장치(ONU) 간의 키 관리 장치 및 방법에 있어서, 상기 광종단장치와 상기 광가입자장치간의 통신설정 과정동안 상기 광종단장치의 공개키를 멀티캐스트하고, 상기 광가입자장치는 이를 수신한 후 상기 광종단장치에게 해당 세션키를 전송함으로써 세션키를 분배하는 장치 및 방법을 제안한다. 또한 세션키 갱신에 있어서, 다중점 제어 프로토콜(MPCP)의 주기적인 일반 게이트 메시지와 광가입자장치의 리포트 메시지를 통해 기존의 키를 새로 생성한 키로 대체한다. 또한 키 복구에 있어서, RSA 공개키 알고리즘의 비밀키 및 공개키 에 오류가 발생했을 경우, 새로운 비밀키 및 공개키 쌍을 생성하여 주기적인 발견 메시지를 통해 공개키를 멀티캐스트함으로써 키복구를 한다. 그리고, 대칭키 알고리즘을 위한 세션키 오류는 광가입자장치의 발견과정에서 할당되는 타임슬롯을 이용하여 생성한 세션키를 리포트 메시지에 포함시켜 광종단장치에 전송함으로써 키를 복구한다. 본 발명에 의하면 EPON 구조에서 기밀성뿐만 아니라 프라이버시 보장 서비스등 보다 향상된 보안 서비스의 제공이 가능하다.

【대표도】

도 5

【색인어】

키 관리, 세션키, 공개키, EPON, MPCP, OLT, ONU

【명세서】

【발명의 명칭】

이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 장치 및 방법{KEY MANAGEMENT DEVICE AND METHOD FOR PROVIDING SECURITY SERVICE IN EPON}

【도면의 간단한 설명】

도 1은 EPON에서 OLT로부터 ONU로 메시지가 하향전송되는 모습을 도시한 도면,

도 2는 EPON에서 ONU로부터 OLT로 메시지가 상향전송되는 모습을 도시한 도면,

도 3은 OLT의 ONU에 대한 발견과정을 이용한 종래의 세션키 분배 과정을 도시한 도면,

도 4는 본 발명의 실시예에 따른 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 장치를 도시한 도면,

도 5는 본 발명의 실시예에 따른 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 방법에서, 세션키 분배과정을 도시한 도면.

* 도면의 주요 부분에 대한 부호의 설명 *

410: 광종단장치(OLT) 420: 비밀키 저장장치

422: 비밀키 저장장치 430,460: 공개키 프로세스

432,462: 공개키 저장장치 440,470: 세션키 프로세스

442,444,472: 세션키 저장장치 450: 광가입자장치(ONU)

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<11> 본 발명은 이더넷 기반 수동형 광네트워크(Ethernet based Passive Optical Network: 이하 'EPON'이라 칭함)에 관한 것으로서, 특히 이더넷 특성상 보안에 취약한 EPON에서 보안 서비스를 제공하기 위해 요구되는 키관리 장치 및 방법에 관한 것이다.

<12> 일반적으로, 수동형 광네트워크(EPON)는 FTTH(Fiber To The Home) 또는 FTTC(Fiber To The Curb/Cabinet) 형태의 가입자 액세스 노드와 광 통신망 단말기(Optical Network Termination) 사이에 수동광분배기(Optical Distribution Network: 이하 'ODN'이라 칭함) 또는 파장분할다중화(Wavelength Division Multiplex: 이하 'WDM'이라 칭함) 소자를 사용하는 구조로서, 모든 노드는 버스나 트리 구조의 형태로 분산된 토폴로지를 갖는다. 이러한 EPON은 다수의 광가입자장치(Optical Network Unit: 이하 'ONU'라 칭함)가 하나의 광섬유를 통해 광종단장치(Optical Line Terminal: 이하 'OLT'라 칭함)를 공유하는 점대다중점(point-to-multipoint) 구조이다. 즉, OLT에서 다수의 ONU로 메시지를 전송하는 하향전송은 브로드캐스팅 방식으로 전달된다. 반면에, 다수의 ONU에서 OLT로 메시지를 전송하는 상향전송은 다중점대점(multipoint-to-point) 방식으로 전달된다.

<13> 현재 인터넷 상의 데이터 트래픽은 1990년 이후 거의 매년 100 퍼센트의 증가율을 보이고 있다. 따라서, 최근 기간망은 파장분할다중화(Wavelength Division Multiplex: 이하 'WDM'이라 칭함) 등의 기술을 이용하여 테라비트 급까지 대역폭이 증가하고 있다. 또한 LAN의 전송속도도 10/100 Mbps 급에서 최대 10 Gbps 까지 증가하고 있다. 따라서, 광대역 서비스를 제공

하기 위한 새로운 가입자망 기술이 요구되고 있고, 이러한 차세대 가입자망으로서 수동형 광네트워크(EPON)가 각광받고 있다.

<14> 도 1은 EPON에서 OLT로부터 ONU로 메시지가 하향전송되는 모습을 도시한 도면이다.

<15> 상기 도 1을 참조하면, 전화국측 광종단장치(OLT)(110)는 광케이블(150)을 통하여 광가입자장치(121, 122, ...,123)에 연결된다. 이 때 상기 광가입자장치(121, 122, ...,123)는 가정 및 회사 등의 내부에 설치되며, 상기 광종단장치(OLT)(110)로부터 인터넷 서비스, 전화 서비스 및 대화형 비디오 서비스 등의 각종 서비스를 제공받게 된다. 이러한 수동형 광네트워크(EPON) 상에서 각종 서비스를 위한 데이터가 포함되는 이더넷 프레임들(140, 141, 142, 143)은 광종단장치(OLT)(110)로부터 스프리터 또는 커플러와 같은 1:N 수동 광분배기(도시되지 않음)를 통하여 각각의 광가입자장치들(121, 122, ...,123)에게 전송된다. 이 때, 각각의 이더넷 프레임(140, 141, 142, 143)은 최대 1,518 바이트까지의 가변길이 패킷으로 구성되고, 목적지 광가입자장치(ONU)에 대한 정보를 포함한다. 이와 같은 패킷들이 광가입자장치들(121, 122, ...,123)에 도착하면, 각각의 광가입자장치(121, 122, ...,123)는 자신에게 해당되지 않는 나머지 패킷들은 버리고, 자신에게 해당하는 패킷만 받아 들인 후, 각각 해당하는 사용자(131, 132, ...,133)에게 전송한다.

<16> 도 2는 EPON에서 ONU로부터 OLT로 메시지가 상향전송되는 모습을 도시한 도면이다.

<17> 상기 도 2를 참조하면, 수동형 광네트워크(EPON) 상에서 상향전송과정은 다음과 같다. 먼저, 다수의 사용자들(131, 132, ...,133)들이 전송하고자 하는 프레임들(211 내지 216)이 각각 해당하는 광가입자장치들(121, 122, ...,123)로 전송된다. 그리고, 상기 광가입자장치들(121, 122, ...,123)은 광종단장치(OLT)(110)로부터 미리 할당받은 각각의 타임슬롯들(221,

222, 223)에 상기 해당하는 프레임들을 실어서 광케이블(150)을 통하여 광종단장치(OLT)(110)로 전송한다.

<18> 이와 같이 수동형 광네트워크(EPON) 상에서, 다수의 광가입자장치들은 하나의 매체(광케이블)를 공유하여 하나의 광종단장치(OLT)과 데이터를 송수신해야 한다. 따라서, 다수의 광가입자장치들(ONU)이 효율적으로 매체접근을 하기 위한 매체접근제어 프로토콜이 요구된다. 이러한 요구에 따라서, EPON에서의 다중점 제어 프로토콜(Multi Point Control Protocol: 이하 'MPCP'라 칭함)은 다수의 광가입자장치들(ONU)과 하나의 광종단장치(OLT) 사이의 상향 데이터를 효율적으로 전송하기 위하여 시분할다중접속(Time Division Multiple Access: 이하 'TDMA'라 칭함) 기반의 메커니즘을 이용한다. 이러한 MPCP의 주요 기능은 광종단장치(OLT)의 광가입자장치(ONU)에 대한 발견과정을 제어하고, 광가입자장치(ONU)에게 타임슬롯을 할당하며, 광종단장치(OLT)와 광가입자장치(ONU)의 시간 기준(Timing Reference)를 제공하는 것이다.

<19> 그러나, 이와 같은 수동형 광네트워크(EPON) 상에서의 데이터 통신 방식은 보안에 취약한 구조를 가지고 있다는 문제가 있다.

<20> 먼저 EPON의 하향 전송과정에서 데이터의 브로드캐스팅 시에 야기되는 보안문제는 다음과 같다. 첫째, 하나의 광종단장치(OLT)에 종속해 있는 모든 광가입자장치(ONU)들은 상기 광종단장치(OLT)의 하향 트래픽을 도청할 수 있다. 둘째, 보안 공격자는 다른 광가입자장치(ONU)의 매체 접근 제어 계층(Medium Access Control: 이하 'MAC'이라 칭함) 주소와 논리 링크 식별자(Logical Link Indentifier: 이하 'LLID'이라 칭함)를 알 수 있다. 셋째, 보안 공격자는 LLID와 MAC 주소를 감시함으로써 다른 광가입자장치(ONU)로 전송되는 트래픽의 양과 종류를 추론할 수 있다. 넷째, 광종단장치(OLT)로부터 브로드캐스팅되는 MPCP 메시지는 각 광가입자장치(ONU)의 상향 트래픽 특성을 노출시킬 수 있다.

<21> 또한, EPON의 상향 전송과정에서 야기되는 보안문제는 다음과 같다. 첫째, 보안 공격자가 다른 광가입자장치(ONU)의 LLID와 MAC 주소를 도용할 수 있다. 둘째, 보안 공격자는 네트워크 자원이나 시스템 관리를 위한 운용관리(Operation and Administration Maintenance: 이하 'OAM'이라 칭함) 정보에 영향을 주는 메시지를 네트워크 상에 폭주시킬 수 있다. 셋째, 보안 공격자가 OAM 채널을 해킹할 경우 EPON 시스템의 구성을 임의로 변경시킬수 있다. 넷째, 광 신호를 전송함으로써 EPON 시스템의 동작을 방해할 수 있다. 다섯째, 반사(reflection)를 이용하여 상향 데이터를 가로챈 후, 이를 수정하여 광종단장치(OLT)에게 전송하는 악의적 보안 공격이 가능하다.

<22> 이와 같은 보안상의 문제를 해결하기 위한 대표적인 예로서, 대한민국 특허등록 번호 제10-2000-0017271호(암호 키 관리 장치 및 방법)에는 하드웨어 자체에 암호화 기능을 추가하여 암호의 유출을 방지하기 위한 장치 및 방법이 개시되어 있다. 또한, 참조논문(Rinat Khoussainov, "LAN Security: problems and solutions for Ethernet networks", Computer Standards & Interfaces, Vol.22, No.2, pp.191-202, 2000.8.1)에는 이더넷에 기반하는 LAN 상에서 전달되는 데이터의 기밀성과 무결성을 보장하기 위한 방법이 개시되어 있다.

<23> 도 3은 OLT의 ONU에 대한 발견과정을 이용한 종래의 세션키 분배 과정을 도시한 도면이다.

<24> 도 3을 참조하면, 먼저 310단계에서, 광종단장치(OLT)는 발견 게이트 메시지(GATE)를 통해 멀티캐스트(dest_addr=multicast)한다. 이 때, 상기 발견 게이트 메시지는 새로운 광가입자장치(ONU)가 등록될 수 있도록 타임슬롯을 할당(GRANT)하고, 자신의 용량(OLT capability), 공개키(KU_{OLT}), 서명(signature)을 위해 자신의 비밀키로 암호화한 임의값($E_{KR_{OLT}}[\text{타임스탬프}]$)을 포함한다.

<25> 320단계에서는, 상기 광가입자장치(ONU)는 상기 발견게이트 메시지에 대한 응답으로서 등록 요청 메시지(REGISTER_REQUEST)를 상기 광종단장치(OLT)에게 전송한다. 이 때, 상기 등록 요청 메시지는 평문으로 된 광가입자장치(ONU)의 임시 MAC 주소(ONU temp. MAC addr.), 광종단장치(OLT)의 공개키로 암호화된 물리계층 ID의 용량(PHY ID capa.), 광가입자장치(ONU)의 용량(ONU capa.), 광종단장치(OLT)의 용량(echo of OLT capa.), 영구 MAC 주소(ONU permanent MAC addr.), 임의적으로 생성된 임시 키(ONU random temporary key)를 포함한다.

<26> 330단계에서는, 상기 광종단장치(OLT)는 상기 광가입자장치(ONU)가 등록되었음을 알리는 등록 메시지(REGISTER)를 상기 광가입자장치(ONU)에게 전송한다. 이 때, 상기 등록 메시지는 평문으로 된 광가입자장치(ONU)의 임시 MAC 주소(ONU temp. MAC addr.), 광가입자장치(ONU)의 임시키로 암호화된 물리계층 ID 목록(PHY ID list), 광가입자장치(ONU)의 용량(echo of ONU capa.), 광가입자장치(ONU)의 영구 MAC 주소(echo of ONU permanent MAC addr.), 128 비트 세션키(128 bit key)를 포함한다.

<27> 340단계에서는, 상기 광종단장치(OLT)는 상기 광가입자장치(ONU)의 상향 전송을 위하여 타임슬롯을 할당하기 위한 일반 게이트 메시지(GATE)를 상기 광가입자장치(ONU)에게 전송한다. 이 때, 상기 일반 게이트 메시지는 평문의 광가입자장치(ONU) 임시 MAC 주소(ONU temp. MAC addr.)와 세션키로 암호화된 타임슬롯 할당 필드(GRANT)를 포함한다.

<28> 마지막으로 350단계에서는, 상기 광가입자장치(ONU)는 등록 메시지에 대한 응답으로서 상기 광종단장치(OLT)에게 등록 확인 메시지(REGISTER_ACK)를 전송한다. 이 때, 상기 등록 확인 메시지에는 세션키로 암호화한 등록된 물리계층 ID(echo of registered PHY ID)가 포함된다.

<29> 그러나, 상술한 종래의 세션키 분배과정은 다음과 같은 문제가 있다. 첫째, 종래의 세션키 분배과정에서의 등록 요청 메시지는 평문으로 된 광가입자장치(ONU)의 임시 MAC 주소(temporary ONU MAC address)와 광종단장치(OLT)의 공개키로 암호화된 광가입자장치(ONU)의 영구 MAC 주소(echo of ONU permanent MAC address)를 포함해야 하기 때문에 비효율적이다. 광가입자장치(ONU)의 임시 MAC 주소는 등록 요청 메시지를 전송하고 OLT로부터 등록 메시지를 수신하기 위해 필요한 주소이다. 그리고, 광가입자장치(ONU)의 영구 MAC 주소는 광가입자장치(ONU)의 발견과정이 성공적으로 처리되고 난 뒤에 영구적으로 사용하게 될 광가입자장치(ONU)의 MAC 주소이다. 이러한 경우에 있어서, 광가입자장치(ONU)는 등록 요청 메시지 중에서 근원지 주소를 제외한 나머지 필드만 광종단장치(OLT)의 공개키로 암호화하기 때문에 프라이버시 보안 서비스를 제공하기 위해서는 근원지 주소로 광가입자장치(ONU) 발견과정에서만 이용되는 임시 MAC 주소를 사용할 수 밖에 없다. 둘째, 광가입자장치(ONU)의 발견과정에서 대칭키 암호 알고리즘을 위해 두 개의 키를 생성해야 하기 때문에 비효율적이다. 하나는 광가입자장치(ONU)의 등록 요청 메시지에 포함되는 임시키(ONU random temporary key)이고, 다른 하나는 광종단장치(OLT)의 등록 메시지에 포함되는 128 비트 세션키(128 bit key)이다. 이와 같은 경우에 있어서, 광가입자장치(ONU) 발견과정에서의 OLT의 등록 메시지는 광가입자장치(ONU)의 임시키로 암호화하고, 광종단장치(OLT)의 일반 게이트 메시지와 광가입자장치(ONU)의 등록 확인 메시지는 128 비트 세션키로 암호화하는 복잡한 구조를 가지게 된다. 셋째, 광가입자장치(ONU)의 등록 요청 메시지에서 광가입자장치(ONU)의 임시 MAC 주소를 제외한 모든 필드를 광종단장치(OLT) 공개키로 암호화해야 하기 때문에 비효율적이다. 공개키 알고리즘은 대칭키 알고리즘에 비하여

암호화 속도가 느리기 때문에, 광가입자장치(ONU)의 임시 MAC 주소를 제외한 나머지 필드를 공개키 알고리즘으로 암호화할 때 성능이 저하된다는 문제가 있다.

【발명이 이루고자 하는 기술적 과제】

<30> 상기와 같은 문제점을 해소하기 위한 본 발명의 목적은 광종단장치(OLT)와 광가입자장치(ONU) 간의 키 관리 장치 및 방법에 있어서, 세션키 분배는 상기 광종단장치(OLT)와 상기 광가입자장치(ONU) 간의 통신설정 과정동안 상기 광종단장치(OLT)의 공개키를 멀티캐스트하고, 상기 광가입자장치(ONU)는 이를 수신한 후 상기 광종단장치(OLT)에게 해당 세션키를 분배하는 장치 및 방법을 제공함에 있다.

<31> 본 발명의 또 다른 목적은 광종단장치(OLT)와 광가입자장치(ONU) 간의 키 관리 방법에 있어서, 세션키 갱신 방법은 다중점 제어 프로토콜의 주기적인 일반 게이트 메시지와 광가입자장치(ONU)의 리포트 메시지를 통해 기존의 키를 새로 생성한 키로 갱신하는 방법을 제공함에 있다.

<32> 본 발명의 또 다른 목적은 광종단장치(OLT)와 광가입자장치(ONU) 간의 키 관리 방법에 있어서, 키 복구 방법은 RSA 공개키 알고리즘의 비밀키 및 공개키에 오류가 발생했을 경우 새로운 비밀키 및 공개키 쌍을 생성하여 주기적인 발견 게이트 메시지를 통해 공개키를 멀티캐스트함으로써 키 복구를 수행하는 방법과, 대칭키 알고리즘을 위한 세션키 오류는 광가입자장치(ONU)의 발견과정에서 할당되는 타임슬롯을 이용하여 생성한 리포트 메시지에 포함시켜 광종단장치(OLT)에 전송함으로써 키 복구를 수행하는 방법을 제공함에 있다.

【발명의 구성 및 작용】

<33> 상기 목적을 달성하기 위한 본 발명에 따른 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 장치는, 데이터를 전송할 광가입자장치를 발견하기 위하여 발견 게이트 메시지를 전송한 후 상기 발견 게이트 메시지를 수신한 상기 광가입자장치로부터 데이터 통신을 요구받는 경우에, 상기 광가입자장치에게 상기 광가입자장치가 등록되었음을 알리기 위하여 상기 광가입자 장치의 영구 MAC 주소가 포함되고 암호화된 등록메시지와 상기 광가입자장치에게 타임슬롯을 할당하기 위하여 상기 광가입자 장치의 영구 MAC 주소가 포함되고 암호화된 일반 게이트 메시지를 전송하는 광종단장치와, 상기 발견 게이트 메시지를 수신한 후, 상기 광종단장치와의 데이터 통신을 하기 위하여 암호화된 등록요청메시지와 상기 등록 메시지에 대한 응답을 위하여 암호화된 등록 확인 메시지를 상기 광종단장치에게 전송하는 광가입자장치를 포함하는 것을 특징으로 한다.

<34> 또한, 본 발명에 따른 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 광종단장치와 광가입자장치간 세션키 분배방법은, 상기 광종단장치는 데이터를 전송할 상기 광가입자장치를 발견하기 위하여 발견 게이트 메시지를 전송하는 과정과, 상기 발견 게이트 메시지를 수신한 상기 광가입자장치는 상기 광종단장치와 데이터 통신을 하기 위하여 암호화된 등록요청메시지를 전송하는 과정과, 상기 광종단장치는 상기 광가입자장치가 등록되었음을 알리는 암호화된 등록메시지를 전송하는 과정과, 상기 광종단장치는 상기 광가입자장치에게 타임슬롯을 할당하기 위하여 암호화된 일반 게이트 메시지를 전송하는 과정과, 상기 광가입자장치는 상기 광종단장치에게 등록메시지에 대한 응답을 위하여 암호화된 등록 확인 메시지를 전송하는 과정을 포함하는 것을 특징으로 한다.

<35> 또한, 본 발명에 따른 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 광종단장치와 광가입자장치간 세션키 갱신방법은, 상기 광종단장치는 미리 정해진 키 갱신 주기에 의하여 상기 광가입자장치에게 키 갱신 정보를 전송하는 과정과, 상기 키 갱신 정보를 수신한 상기 광가입자장치는 새로 생성한 세션키를 상기 광종단장치에게 전송하는 과정을 포함하는 것을 특징으로 한다.

<36> 또한, 본 발명에 따른 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 광종단장치와 광가입자장치간 키 복구 방법은, 비밀키 및 공개키 쌍에 오류 발생 여부를 판단하는 과정과, 상기 비밀키 및 공개키 쌍에 오류 발생한 경우에는 상기 광종단장치는 비밀키 및 공개키 쌍을 새로 생성하고, 상기 새로 생성된 공개키를 포함한 메시지를 이용하여 멀티캐스트하는 과정과, 상기 광가입자장치는 상기 광종단장치의 새로 생성된 공개키를 수신한 후, 상기 새로 생성된 공개키와 상기 광가입자장치에 미리 저장되어 있는 공개키를 서로 비교하여, 상기 새로 생성된 공개키와 상기 광가입자장치에 미리 저장되어 있는 공개키가 서로 같으면 상기 새로 생성된 공개키를 폐기하고, 상기 새로 생성된 공개키와 상기 광가입자장치에 미리 저장되어 있는 공개키가 서로 다르면 상기 새로 생성된 공개키를 상기 광가입자장치의 공개키 저장장치에 저장하는 과정을 포함하는 것을 특징으로 한다.

<37> 또한 본 발명에 따른 또다른 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 광종단장치와 광가입자장치간 키 복구 방법은, 상기 광종단장치와 상기 광가입자장치 사이에 세션키 오류 발생여부를 판단하는 과정과, 상기 광종단장치와 상기 광가입자장치 사이에 세션키 오류가 발생한 경우에 상기 광가입자장치는 발견 게이트 메시지와 함께 전송된 타임슬롯을 이용하여 새로 생성한 세션키를 상기 광종단장치에 전송하는 과정을 포함하는 것을 특징으로 한다.

<38> 이하 본 발명의 바람직한 실시예의 상세한 설명이 첨부된 도면들을 참조하여 설명될 것이다. 도면들 중 참조번호 및 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 참조번호들 및 부호들로 나타내고 있음에 유의해야 한다. 하기에서 본 발명을 설명함에 있어, 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다.

<39> 도 4는 본 발명의 실시예에 따른 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 장치를 도시한 도면이다.

<40> 도 4를 참조하면, 상호 키분배를 위해 본 발명에 따른 광종단장치(OLT)(410)는 MAC 제어 클라이언트(411)와, MAC 제어부(412)를, 광가입자장치(ONU)(450)는 MAC 제어 클라이언트(451)와, MAC 제어부(452)를 포함한다.

<41> 상기 광종단장치(OLT) 내 MAC 제어 클라이언트(411)는 계층 2 스위칭 기능과 계층 3 응용프로그램 인터페이스(Application Program Interface: 이하 'API'라 칭함) 기능을 한다. 상기 광종단장치(OLT) 내 MAC 제어 클라이언트(411)는 점대다중점(point-to-multipoint) 통신을 담당하는 모듈로서 다중(multi) 광가입자장치(ONU) 인터페이스를 처리한다. 상기 광가입자장치(ONU) 내 MAC 제어 클라이언트(451)는 계층 2 스위칭 기능을 하는 API로서, 상기 광종단장치(OLT)(410)와 점대점(point-to-point) 통신을 담당하는 모듈이다. 그리고 MAC 제어부(412, 452)는 매체 접근 제어 계층(Medium Access Control: MAC)(413, 453)에 대하여 가입자로부터 입력되는 매체 접근 제어 기능을 담당한다. 물리계층(PHY)(414, 454)은 광섬유 또는 연선(twisted pair)과 같은 물리적 전송매체 접속점이다.

<42> 이하에서는 본 발명에 따른 키관리 장치의 동작 및 구성을 상세히 설명한다. 광종단장치(OLT)(410)는 주기적으로 발견 게이트 메시지를 통해 공개키를 멀티캐스트한다. 그리고, 광가

입자장치(ONU)(450)는 등록 요청 메시지와 등록 확인 메시지를 세션키로 암호화하며, 이와 같이 세션키로 암호화된 메시지들을 복호하기 위한 세션키는 광종단장치(OLT)(410)의 공개키로 암호화하여 광종단장치(OLT)(410)로 전송된다. 이와 같은 경우에, 상기 광종단장치(OLT)(410)는 상기 광가입자장치(ONU)(450)로부터 수신한 메시지를 복호하기 위하여 상기 광종단장치(OLT)(410)의 비밀키를 사용해야 한다. 그리고, 상기 비밀키는 상기 공개키를 이용하여 생성된다. 따라서, 상기 광종단장치(OLT) 내의 MAC 제어부(412)는 비밀키의 생성과 상기 비밀키에 대하여 암호화 및 복호화를 위한 비밀키 프로세스(420)와 공개키의 생성과 상기 공개키에 대하여 암호화 및 복호화를 위한 공개키 프로세스(430)를 포함한다. 그리고, 상기 광종단장치(OLT)(410) 내의 MAC 제어부(412)는 상기 각각의 비밀키와 공개키를 저장 및 관리하기 위한 비밀키 저장장치(422) 및 공개키 저장장치(432)를 더 포함한다. 또한, 수동형 광네트워크(EPON)은 하나의 광종단장치(OLT)가 다수의 광가입자장치(ONU)들에 대하여 서비스를 제공하는 점대다중점(point-to-multipoint) 구조이므로, 광종단장치(OLT)는 다수의 광가입자장치(ONU)들 각각에 대한 세션키를 관리해야 한다. 따라서, 상기 광종단장치(OLT) 내의 MAC 제어부(412)는 다수의 광가입자장치(ONU)들 각각에 대한 세션키를 보관 및 관리하기 위한 세션키 저장장치(442, ..., 444)들과, 대칭키 알고리즘에 기반하여 상기 세션키에 대한 암호화 및 복호화를 위한 세션키 프로세스(440)을 더 포함한다. 또한, 상기 광종단장치(OLT) 내의 MAC 제어부(412)는 네트워크 상의 지연 정도를 측정하기 위해 전송하는 시간을 보내기 위한 타임스탬프부(TS)(415)와, 상기 타임스탬프부(415)에 클럭을 제공하는 클럭 레지스터(422)와, 메시지의 시작을 표시하기 위한 길이 표시부(Length)(417)를 더 포함한다.

<43> 이에 반하여, 광가입자장치(ONU)(450)는 광종단장치(OLT)(410)와의 관계에 있어서 점대점(point-to-point) 구조를 갖는다. 따라서, 상기 광가입자장치(ONU)

내의 MAC 제어부(452)는 서비스를 제공하고 있는 하나의 광종단장치(OLT)(410)에 대한 공개키의 저장 및 관리하기 위한 공개키 저장장치(462)와, 공개키의 암호화 및 복호화를 위한 공개키 프로세스(460)를 포함한다. 또한, 상기 광가입자장치(ONU) 내의 MAC 제어부(452)는 상기 광종단장치(OLT)(410)와 공유하고 있는 세션키를 저장 및 관리하기 위한 세션키 저장장치(472)와 세션키의 생성과 암호화 및 복호화를 위한 세션키 프로세스(470)를 더 포함한다. 또한, 상기 광가입자장치(ONU) 내의 MAC 제어부(452)는 네트워크 상의 지연 정도를 측정하기 위해 전송하는 시간을 보내기 위한 타임스탬프부(TS)(481)와, 상기 타임스탬프를 저장하기 위한 클럭 레지스터(484)와, 메시지의 시작을 표시하기 위한 스타트 표시부(Start)(482)와 이를 저장하기 위한 스타트 레지스터(485)와, 메시지의 길이를 표시하기 위한 길이 표시부(Length)(483)와 이를 저장하기 위한 길이 레지스터(486), 및 전송관리를 위한 대역폭 할당부(487)를 더 포함한다. 여기서 상기 대역폭 할당부(487)는 타임스탬프, 스타트 및 길이 정보를 이용하여 대역폭을 할당한 후 상기 광종단장치(OLT)(410)로 전송하는 역할을 한다.

<44> 도 5는 본 발명의 실시예에 따른 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 방법에서, 세션키 분배과정을 도시한 도면이다.

<45> 도 5를 참조하면, 먼저 510단계에서, 광종단장치(OLT)는 목적지 광가입자장치(ONU)의 발견과정을 수행하기 위해 평문의 발견 게이트 메시지(GATE)를 주기적으로 멀티캐스트(dest_addr=multicast)한다. 이 때, 상기 발견 게이트 메시지는 새로운 광가입자장치(ONU)가 등록될 수 있도록 타임슬롯을 할당(GRANT)하고, 자신(OLT)의 용량(OLT capability), 공개키(KU_{OLT}), 서명(signature)을 위해 자신(OLT)의 비밀키로 암호화한 임의값(타임스탬프)($E_{KR_{olt}}[N1]$)을 포함한다.

<46> 520단계에서는, 새로운 목적지 광가입자장치(ONU)가 상기 발견 게이트 메시지를 수신하면, 상기 광가입자장치(ONU)는 상기 발견게이트 메시지에 대한 응답으로서 등록 요청 메시지(REGISTER_REQUEST)를 상기 광종단장치(OLT)에게 전송한다. 이 때, 상기 등록 요청 메시지는 물리계층 ID의 용량(PHY ID capa.), 상기 광가입자장치(ONU)의 용량(ONU capa.), 상기 광종단장치(OLT)의 용량(echo of OLT capa.), 광종단장치(OLT)의 공개키로 암호화한 세션키($E_{KU_{olt}}[\text{세션키}]$), 상기 광종단장치(OLT)의 공개키로 복호한 임의값(N1), 상기 광가입자장치(ONU)의 서명을 위해 생성한 임의값(N2)을 포함한다. 그리고, 상기 등록 요청 메시지 중 상기 광종단장치(OLT)의 공개키로 암호화한 세션키를 제외한 나머지 모든 필드는 세션키로 암호화된다.

<47> 530단계에서는, 상기 광종단장치(OLT)는 상기 광가입자장치(ONU)로부터 수신한 등록 요청 메시지를 세션키로 복호한 후, 상기 광가입자장치(ONU)가 등록되었음을 알리는 등록 메시지(REGISTER)를 상기 광가입자장치(ONU)에게 전송한다.

<48> 이 때, 상기 등록 메시지는 상기 광가입자 장치(ONU)의 영구 MAC 주소(dest_addr=ONU MAC addr)와, 물리계층 ID 목록(PHY ID list), 상기 광가입자장치(ONU)의 용량(echo of ONU capa.), 상기 광가입자장치(ONU)의 서명(N2)을 포함한다.

<49> 540단계에서는, 상기 광종단장치(OLT)는 광가입자장치(ONU)의 상향 전송을 위하여 일반 게이트 메시지(GATE)를 상기 광가입자장치(ONU)에게 전송한다. 이 때, 상기 일반 게이트 메시지는 상기 광가입자 장치(ONU)의 영구 MAC 주소(dest_addr=ONU MAC addr)와, 타임슬롯을 할당하기 위한 타임슬롯 할당 필드(GRANT)를 포함하고, 상기 일반 게이트 메시지는 세션키로 암호화된다.

<50> 마지막으로 550단계에서는, 상기 광가입자장치(ONU)는 등록 메시지에 대한 응답으로서 상기 광종단장치(OLT)에게 등록 확인 메시지(REGISTER_ACK)를 전송한다.

<51> 이 때, 상기 등록 확인 메시지는 상기 광종단장치(OLT)의 공개키로 암호화한 세션키($E_{KU_{olt}}$[세션키])와 등록된 물리계층 ID(echo of registered PHY ID)를 포함하며, 상기 등록 확인 메시지는 세션키로 암호화되어 상기 광종단장치(OLT)에게 전달된다.

<52> 이와 같은 방법에 의하여 본 발명의 실시예에 따른 세션키 분배가 이루어지게 된다. 그러고, 더 나아가 본 발명의 실시예에서는 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 방법에서는 주기적인 세션키 갱신 방법과 데이터 전송시 오류가 발생한 경우에 있어서 세션키 복구 방법을 더 제안한다.

<53> 본 발명의 실시예에 따른 세션키 갱신 방법을 도 4를 참조하여 상술하면 다음과 같다. 우선, 광종단장치(OLT)(410)는 광가입자장치(ONU)(450)에게 타임슬롯을 할당하기 위하여 주기적으로 일반 게이트 메시지를 상기 광가입자장치(ONU)(450)에게 전송한다. 그리고, 상기 광가입자장치(ONU)(450)는 상향 전송용 메시지인 리포트 메시지(REPORT)를 통하여 상기 광종단장치(OLT)(410)에게 대역폭 할당을 요구할 수 있다. 본 발명의 실시예에서는 이와 같은 수동형 광네트워크(EPON)의 특성을 이용함으로써 상기 광종단장치(OLT)(410)와 상기 광가입자장치(ONU)(450) 사이에 세션키를 갱신하는 방법을 제안한다. 먼저, 상기 광종단장치(OLT)(410)는 미리 정해진 키 갱신 주기를 고려하여, 주기적으로 일반 게이트 메시지를 통하여 상기 광가입자장치(ONU)(450)에게 세션키를 갱신할 것을 알리고, 상기 광가입자장치(ONU)(450)는 리포트 메시지(REPROT)를 통하여 새로 생성한 세션키를 상기 광종단장치(OLT)(410)에게 전송한다. 그리고, 상기 광종단장치(OLT)(410)는 상기 광가입자장치(ONU)(450)로부터 수신한 새로운 세션키를 내부의 세션키 저장장치들(442, ..., 444) 중 해당하는 세션키 저장장치에 저장하여 관리하

며, 상기 광가입자장치(ONU)(450)는 새로 생성한 세션키를 자신의 세션키 저장장치(472)에 저장하여 관리한다. 이 때, 수동형 광네트워크(EPON)는 키 분배를 위하여 RSA 공개키 알고리즘을 사용하고, 데이터의 암호화는 대칭키 알고리즘을 사용한다. 또한, 상기 광종단장치(OLT)(410)는 공개키를 분배하고, 상기 광가입자장치(ONU)(450)는 세션키를 분배한다. 이와 같은 방법에 의하여 상기 광종단장치(OLT)(410)와 상기 광가입자장치(ONU)(450) 사이에 세션키의 갱신이 가능하게 된다.

<54> 그러나, 이와 같은 과정에서 전송 오류에 의한 상기 광종단장치(OLT)(410)와 상기 광가입자장치(ONU)(450) 사이에 키 값의 손실이 발생할 수 있다. 상기 광종단장치(OLT)(410)와 상기 광가입자장치(ONU)(450) 사이에 비밀키 및 공개키 쌍의 오류와 세션키 오류는 다음과 같은 경우에 발생한다. 먼저, RSA 공개키 알고리즘의 비밀키 및 공개키 오류는 광종단장치(OLT)(410)의 공개키를 포함하는 발견 게이트 메시지가 광가입자장치(ONU)(450)에게 전송되는 과정에서 전송오류가 발생할 수 있다. 또한, 상기 광가입자장치(ONU)(450)의 동작 오류가 발생할때에도 광종단장치(OLT)(410)와 광가입자장치(ONU)(450) 사이에 잘못된 비밀키 및 공개키 쌍을 가질 수도 있다. 다음으로, 대칭키 암호 알고리즘을 위한 세션키 오류는, 상기 광종단장치(OLT)(410)가 상기 광가입자장치(ONU)(450)을 발견하는 과정에서 등록 요청 메시지가 전송되는 중에 발생하는 경우, 상기 광종단장치(OLT)(410)의 동작 오류가 발생할 때 상기 광종단장치(OLT)(410)와 상기 광가입자장치(ONU)(450) 사이에 세션키 오류가 발생하는 경우, 상기 광종단장치(OLT)(410)가 상기 광가입자장치(ONU)(450)에게 타임슬롯을 할당하기 위한 과정에서 상기 광가입자장치(ONU)(450)의 리포트 메시지에 전송호류가 발생하는 경우 및 상기 광종단장치(OLT)(410)의 동작 오류에 의해서 상기 광종단장치(OLT)(410)와 상기 광가입자장치(ONU)(450) 사이에 세션키 오류가 발생하는 경우에 발생할 수 있다.

<55> 이와 같이 수동형 광네트워크(EPON)에서 비밀키 및 공개키 쌍의 오류와 세션키 오류가 발생한 경우에 있어서, 광종단장치(OLT)와 광가입자장치(ONU)간 키 복구 방법을 도 4 및 도 5를 참조하여 상술하면 다음과 같다.

<56> 먼저, 수동형 광네트워크(EPON)에서 비밀키 및 공개키 쌍의 오류가 발생한 경우에 있어서, 광종단장치(OLT)와 광가입자장치(ONU)간 키 복구 방법을 상술한다.

<57> 우선, 광종단장치(OLT)(410) 또는 광가입자장치(ONU)(450)는 비밀키 및 공개키 쌍의 오류발생 여부를 판단한다. 이와 같은 비밀키 및 공개키 쌍의 오류는 광종단장치(OLT)(410) 또는 광가입자장치(ONU)(450) 각각에 수신된 메시지를 세션키로 복호한 후에 프레임 체크 시퀀스(Frame Check Sequence: 이하 'FCS'라 칭함)를 검사함으로써 비밀키 및 공개키 오류를 발견할 수 있다. 이 때, 비밀키 및 공개키 오류가 발생한 경우에는 상기 광종단장치(OLT)(410)는 비밀키 및 공개키 쌍을 새로 생성한다. 그리고, 상기 광종단장치(OLT)(410)는 발견 게이트 메시지에 상기 새로 생성한 상기 광종단장치(OLT)(410)의 공개키를 포함시켜 멀티캐스트한다. 이후에 상기 새로 생성된 공개키가 포함된 발견 게이트 메시지를 수신한 상기 광가입자장치(ONU)(450)는 상기 광종단장치(OLT)(410)의 새로 생성된 공개키와 상기 광가입자장치(ONU)(450) 내부의 공개키 저장장치(462)에 미리 저장되어 있던 상기 광종단장치(OLT)(410)의 공개키를 서로 비교한다. 그리고, 상기 광가입자장치(ONU)(450)는 상기 비교한 결과, 새로 생성된 공개키와 미리 저장되어 있던 공개키가 서로 같으면 상기 새로 생성된 공개키를 폐기하고, 서로 다르면 상기 새로 생성된 공개키를 상기 광가입자장치(ONU)(450) 내부의 공개키 저장장치(462)에 저장함으로써 키 복구가 이루어진다.

<58> 다음으로, 수동형 광네트워크(EPON)에서 세션키 오류가 발생한 경우에 있어서, 광종단장치(OLT)와 광가입자장치(ONU)간 키 복구 방법을 상술한다.

<59> 우선, 광종단장치(OLT)(410) 또는 광가입자장치(ONU)(450)는 세션키 오류발생 여부를 판단한다. 이와 같이 발생하는 세션키 오류는 상기 광종단장치(OLT)(410)가 미리 타임슬롯을 할당한 광가입자장치(ONU)(450)로부터 지속적으로 어떠한 상향 전송도 없을 경우에 오류가 발생하였다고 판단할 수 있다. 그 이유는 세션키 오류가 발생한 경우에는 상기 광가입자장치(ONU)(450)는 일반 게이트 메시지를 복호할 수 없게 되므로, 상기 광가입자장치(ONU)(450)가 상기 광종단장치(OLT)(410)로부터 타임슬롯을 할당받았음에도 불구하고 상향 전송을 하지 못하고 있기 때문이다. 그리고, 상기 광가입자장치(ONU)(450)가 상기 광종단장치(OLT)(410)으로부터 주기적으로 전송되는 발견 게이트 메시지는 수신하지만, 일반 게이트 메시지를 지속적으로 수신하지 못하는 경우에도 상기 광가입자장치(ONU)(450)와 상기 광종단장치(OLT)(410) 사이에 세션키 오류가 발생하였음을 판단할 수 있다. 이와 같이 세션키 오류가 발생하면 상기 광가입자장치(ONU)(450)는 상기 광종단장치(OLT)(410)으로부터 일반 게이트 메시지를 수신할 수 없기 때문에 정상적인 타임 슬롯을 할당 받을 수 없다. 따라서, 상기 광가입자장치(ONU)(450)는 상기 광종단장치(OLT)(410)가 새로운 광가입자장치(ONU)의 발견과정에서 발견 게이트 메시지를 통하여 할당되는 타임슬롯을 이용하여 새로 생성한 세션키를 리포트 메시지에 포함시켜 상기 광종단장치(OLT)(410)에게 전송함으로써 세션키를 복구할 수 있게 된다.

<60> 한편 본 발명의 상세한 설명에서는 구체적인 실시예에 관해 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능함은 물론이다. 그러므로 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 안되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

【발명의 효과】

<61> 이상에서 상술한 바와 같이 본 발명에 따른 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 장치 및 방법은 다음과 같은 효과가 있다.

<62> 첫째, 키 관리 장치 및 키 관리 방법을 용이하게 구현할 수 있다. 키 관리를 위한 과정에서 OLT의 발견 게이트 메시지를 제외한 모든 MPCP 메시지의 전체 필드를 암호화함으로써 ONU는 하나의 영구 MAC 주소만 사용할 수 있으므로, 불필요한 주소 공간의 낭비를 줄이고 임시 MAC 주소와 영구 MAC 주소의 매핑 과정으로 생략할 수 있어 키 관리 장치가 간단하고 키 관리 방법의 구현이 용이하다. 특히, 새로운 ONU는 발견 게이트 메시지를 수신할 때 OLT와 ONU 간의 암호화를 위해 사용할 세션키를 생성한 후 등록 요청메시지에 포함시켜 OLT 에게 분배함으로써, ONU가 생성하여 분배하는 임시키와 OLT가 생성하여 분배하는 세션키를 별도로 관리하던 종래의 방법보다 암호화 구조를 단순화 시킬 수 있다.

<63> 둘째, 메시지의 암호화 성능을 향상시킬 수 있다. 본 발명에 따른 키 관리 장치 및 방법에 의하면, 상향 전달과정의 세션키 필드를 제외한 모든 메시지를 대칭키 알고리즘으로 암호화하기 때문에 보다 향상된 암호화 성능을 제공할 수 있다.

<64> 셋째, 보다 향상된 보안 서비스를 제공할 수 있다. OLT의 발견 게이트 메시지를 제외한 나머지 MCPC 메시지의 전체 필드를 암호화함으로써 기밀성 서비스 뿐만 아니라 프라이버시 서비스도 제공할 수 있게 된다.

<65> 넷째, 세션키 분배 방법외에 세션키 갱신 방법 및 세션키 복구 방법을 제공함으로써 보다 향상된 키 관리가 가능하다.

【특허청구범위】

【청구항 1】

이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 장치에 있어서,

데이터를 전송할 광가입자장치를 발견하기 위하여 발견 게이트 메시지를 전송한 후 상기 발견 게이트 메시지를 수신한 상기 광가입자장치로부터 데이터 통신을 요구받는 경우에, 상기 광가입자장치에게 상기 광가입자장치가 등록되었음을 알리기 위하여 상기 광가입자 장치의 영구 MAC 주소가 포함되고 암호화된 등록메시지와 상기 광가입자장치에게 타임슬롯을 할당하기 위하여 상기 광가입자 장치의 영구 MAC 주소가 포함되고 암호화된 일반 게이트 메시지를 전송하는 광종단장치와,

상기 발견 게이트 메시지를 수신한 후, 상기 광종단장치와의 데이터 통신을 하기 위하여 암호화된 등록요청메시지와 상기 등록 메시지에 대한 응답을 위하여 암호화된 등록 확인 메시지를 상기 광종단장치에게 전송하는 광가입자장치를 포함하는 것을 특징으로 하는 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 장치.

【청구항 2】

제 1항에 있어서, 상기 발견 게이트 메시지는 주기적으로 전송되는 것을 특징으로 하는 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 장치.

【청구항 3】

제 1항 또는 제 2항에 있어서, 상기 발견 게이트 메시지는 상기 광가입자장치가 등록될 수 있도록 할당된 타임슬롯과, 상기 광종단장치의 용량과, 공개키와, 서명을 위해 상기 광종단

장치의 비밀키로 암호화된 임의값을 포함하는 것을 특징으로 하는 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 장치.

【청구항 4】

제 1항에 있어서, 상기 등록 요청 메시지는 물리계층 ID와, 상기 광가입자장치의 용량과, 세션키와, 상기 광종단장치의 공개키로 복호한 임의값과, 상기 광가입자장치의 서명을 위해 생성한 임의값을 포함하는 것을 특징으로 하는 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 장치.

【청구항 5】

제 4항에 있어서, 상기 물리계층 ID와, 상기 광가입자장치의 용량과, 상기 광종단장치의 공개키로 복호한 임의값과, 상기 광가입자장치의 서명을 위해 생성한 임의값은 세션키로 암호화되는 것을 특징으로 하는 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 장치.

【청구항 6】

제 4항에 있어서, 상기 세션키는 상기 광종단장치의 공개키로 암호화되는 것을 특징으로 하는 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 장치.

【청구항 7】

제 1항에 있어서, 상기 등록 메시지는 물리계층 ID 목록과, 상기 광가입자장치의 용량과, 상기 광가입자장치의 서명을 더 포함하는 것을 특징으로 하는 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 장치.

【청구항 8】

제 1항에 있어서, 상기 일반 게이트 메시지는 상기 광가입자장치의 상향 전송을 위한 타임슬롯 할당 필드를 더 포함하는 것을 특징으로 하는 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 장치.

【청구항 9】

제 8항에 있어서, 상기 일반 게이트 메시지는 세션키로 암호화되는 것을 특징으로 하는 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 장치.

【청구항 10】

제 1항에 있어서, 상기 등록 확인 메시지는 상기 광종단장치의 공개키로 암호화한 세션키를 포함하는 것을 특징으로 하는 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 장치.

【청구항 11】

제 10항에 있어서, 상기 등록 확인 메시지는 세션키로 암호화되는 것을 특징으로 하는 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 장치.

【청구항 12】

제 1항에 있어서, 상기 광종단장치는,

데이터를 통신할 광가입자장치를 발견하기 위하여 전송하는 발견 게이트 메시지에 포함될 공개키를 생성하고, 상기 공개키에 대한 암호화 및 복호화를 위한 공개키 프로세스와,

상기 광가입자장치를 발견한 후, 상기 광가입자장치로부터 세션키로 암호화 되어 수신되는 등록 요청 메시지와 등록 확인 메시지를 복호하고, 상기 광가입자장치에게 타임슬롯을 할당하기 위하여 전송하는 일반 게이트 메시지와 상기 광가입자장치가 등록되었음을 알리는 등록 메시지를 세션키로 암호화하기 위한 세션키 프로세스와,

상기 공개키를 이용하여 생성되며 상기 광가입자장치와 메시지를 암호화하여 송수신하기 위한 비밀키를 생성하고, 상기 비밀키에 대한 암호화 및 복호화를 위한 비밀키 프로세스와,

상기 공개키와 상기 세션키와 상기 비밀키를 저장 및 관리하기 위한 저장수단을 포함하는 것을 특징으로 하는 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 장치.

【청구항 13】

제 1항에 있어서, 상기 광가입자장치는,

광종단장치로부터 발견 게이트 메시지를 수신하는 경우에, 상기 광종단장치와의 암호화된 통신을 위하여 세션키를 생성하고, 상기 광종단장치에게 등록요청을 위하여 전송하는 등록요청 메시지의 일부를 세션키로 암호화 하고, 상기 광종단장치로부터 수신되는 등록을 알리는 등록 메시지와 타임슬롯 할당을 위한 일반 게이트 메시지를 세션키로 복호하고, 상기 등록 메시지에 대한 등록 확인을 위하여 전송하는 등록 확인 메시지를 세션키로 암호화하기 위한 세션키 프로세스와,

상기 세션키를 상기 광종단장치로부터 수신한 공개키로 암호화하기 위한 공개키 프로세스와,

상기 세션키 및 상기 공개키를 저장하기 위한 저장수단을 포함하는 것을 특징으로 하는 이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 장치.

【청구항 14】

이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 키관리 방법에서, 광종단장치와 광가입자장치간 세션키 분배방법에 있어서,

상기 광종단장치는 데이터를 전송할 상기 광가입자장치를 발견하기 위하여 발견 게이트 메시지를 전송하는 과정과,

상기 발견 게이트 메시지를 수신한 상기 광가입자장치는 상기 광종단장치와 데이터 통신을 하기 위하여 암호화된 등록요청메시지를 전송하는 과정과,

상기 광종단장치는 상기 광가입자장치가 등록되었음을 알리기 위하여 상기 광가입자 장치의 영구 MAC 주소가 포함되고 암호화된 등록메시지를 전송하는 과정과,

상기 광종단장치는 상기 광가입자장치에게 타임슬롯을 할당하기 위하여 상기 광가입자 장치의 영구 MAC 주소가 포함되고 암호화된 일반 게이트 메시지를 전송하는 과정과,

상기 광가입자장치는 상기 광종단장치에게 등록메시지에 대한 응답을 위하여 암호화된 등록 확인 메시지를 전송하는 과정을 포함하는 것을 특징으로 하는 광종단장치와 광가입자장치 간 세션키 분배방법.

【청구항 15】

제 14항에 있어서, 상기 발견 게이트 메시지는 주기적으로 전송되는 것을 특징으로 하는 광종단장치와 광가입자장치간 세션키 분배방법.

【청구항 16】

제 14항 또는 제 15항에 있어서, 상기 발견 게이트 메시지는 상기 광가입자장치가 등록될 수 있도록 할당된 타임슬롯과, 상기 광종단장치의 용량과, 공개키와, 서명을 위해 상기 광종단장치의 비밀키로 암호화된 임의값을 포함하는 것을 특징으로 하는 광종단장치와 광가입자장치간 세션키 분배방법.

【청구항 17】

제 14항에 있어서, 상기 등록 요청 메시지는 물리계층 ID와, 상기 광가입자장치의 용량과, 세션키와, 상기 광종단장치의 공개키로 복호한 임의값과, 상기 광가입자장치의 서명을 위해 생성한 임의값을 포함하는 것을 특징으로 하는 광종단장치와 광가입자장치간 세션키 분배방법.

【청구항 18】

제 17항에 있어서, 상기 물리계층 ID와, 상기 광가입자장치의 용량과, 상기 광종단장치의 공개키로 복호한 임의값과, 상기 광가입자장치의 서명을 위해 생성한 임의값은 세션키로 암호화되는 것을 특징으로 하는 광종단장치와 광가입자장치간 세션키 분배방법.

【청구항 19】

제 17항에 있어서, 상기 세션키는 상기 광종단장치의 공개키로 암호화되는 것을 특징으로 하는 광종단장치와 광가입자장치간 세션키 분배방법.

【청구항 20】

제 14항에 있어서, 상기 등록 메시지는 물리계층 ID 목록과, 상기 광가입자장치의 용량과, 상기 광가입자장치의 서명을 더 포함하는 것을 특징으로 하는 광종단장치와 광가입자장치간 세션키 분배방법.

【청구항 21】

제 14항에 있어서, 상기 일반 게이트 메시지는 상기 광가입자장치의 상향 전송을 위한 타임슬롯 할당 필드를 더 포함하는 것을 특징으로 하는 광종단장치와 광가입자장치간 세션키 분배방법.

【청구항 22】

제 21항에 있어서, 상기 일반 게이트 메시지는 세션키로 암호화되는 것을 특징으로 하는 광종단장치와 광가입자장치간 세션키 분배방법.

【청구항 23】

제 14항에 있어서, 상기 등록 확인 메시지는 상기 광종단장치의 공개키로 암호화한 세션키를 포함하는 것을 특징으로 하는 광종단장치와 광가입자장치간 세션키 분배방법.

【청구항 24】

제 23항에 있어서, 상기 등록 확인 메시지는 세션키로 암호화되는 것을 특징으로 하는 광종단장치와 광가입자장치간 세션키 분배방법.

【청구항 25】

이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 광종단장치와 광가입자장치간 세션키 갱신방법에 있어서,

상기 광종단장치는 미리 정해진 키 갱신 주기에 의하여 상기 광가입자장치에게 키 갱신 정보를 전송하는 과정과,

상기 키 갱신 정보를 수신한 상기 광가입자장치는 새로 생성한 세션키를 상기 광종단장치에게 전송하는 과정을 포함하는 것을 특징으로 하는 광종단장치와 광가입자장치간 세션키 갱신방법.

【청구항 26】

제 25항에 있어서, 상기 광종단장치는 상기 광가입자장치의 세션키를 상기 광가입자장치의 세션키에 할당된 저장장치에 보관하는 과정과,

상기 광가입자장치는 세션키를 상기 광가입자장치 내부의 세션키 저장장치에 저장하는 과정을 더 포함함을 특징으로 하는 광종단장치와 광가입자장치간 세션키 갱신방법.

【청구항 27】

제 25항에 있어서, 상기 키 갱신 정보는 일반 게이트 메시지를 통하여 상기 광가입자장치에게 전송되는 것을 특징으로 하는 광종단장치와 광가입자장치간 세션키 갱신방법.

【청구항 28】

제 25항에 있어서, 상기 새로 생성한 세션키는 리포트 메시지를 통하여 상기 광종단장치에게 전송되는 것을 특징으로 하는 광종단장치와 광가입자장치간 세션키 갱신방법.

【청구항 29】

이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 광종단장치와 광가입자장치간 키 복구 방법에 있어서,

비밀키 및 공개키 쌍에 오류 발생 여부를 판단하는 과정과,

상기 비밀키 및 공개키 쌍에 오류 발생한 경우에는 상기 광종단장치는 비밀키 및 공개키 쌍을 새로 생성하고, 상기 새로 생성된 공개키를 포함한 메시지를 이용하여 멀티캐스트하는 과정과,

상기 광가입자장치는 상기 광종단장치의 새로 생성된 공개키를 수신한 후, 상기 새로 생성된 공개키와 상기 광가입자장치에 미리 저장되어 있는 공개키를 서로 비교하여, 상기 새로 생성된 공개키와 상기 광가입자장치에 미리 저장되어 있는 공개키가 서로 같으면 상기 새로 생성된 공개키를 폐기하고, 상기 새로 생성된 공개키와 상기 광가입자장치에 미리 저장되어 있는 공개키가 서로 다르면 상기 새로 생성된 공개키를 상기 광가입자장치의 공개키 저장장치에 저장하는 과정을 포함하는 것을 특징으로 하는 광종단장치와 광가입자장치간 키 복구 방법.

【청구항 30】

제 29항에 있어서, 비밀키 및 공개키 쌍에 오류 발생 여부를 판단하는 과정은, 상기 광종단장치 또는 상기 광가입자장치가 수신된 메시지를 세션키로 복호한 후에 프레임 체크 시퀀스(FCS)를 검사하여 오류 발생여부를 판단하는 것을 특징으로 하는 광종단장치와 광가입자장치간 키 복구 방법.

【청구항 31】

제 29항에 있어서, 상기 광종단장치가 새로 생성한 공개키는 발견 게이트 메시지에 실어져서 상기 광가입자장치로 전송되는 것을 특징으로 하는 광종단장치와 광가입자장치간 키 복구 방법.

【청구항 32】

이더넷 기반 수동형 광네트워크의 보안서비스 제공을 위한 광종단장치와 광가입자장치간 키 복구 방법에 있어서,

상기 광종단장치와 상기 광가입자장치 사이에 세션키 오류 발생여부를 판단하는 과정과,

상기 광종단장치와 상기 광가입자장치 사이에 세션키 오류가 발생한 경우에 상기 광가입자장치는 발견 게이트 메시지에 실어져서 전송된 타임슬롯을 이용하여 새로 생성한 세션키를 상기 광종단장치에 전송하는 과정을 포함하는 것을 특징으로 하는 광종단장치와 광가입자장치간 키 복구 방법.

【청구항 33】

제 32항에 있어서, 상기 세션키 오류 발생여부를 판단하는 과정은,

상기 광종단장치가 타임슬롯을 할당한 광가입자장치로부터 지속적으로 어떠한 상향 전송도 없으면 세션키 오류가 발생한 것으로 판단하는 것을 특징으로 하는 광종단장치와 광가입자

장치간 키 복구 방법.

【청구항 34】

제 32항에 있어서, 상기 세션키 오류 발생여부를 판단하는 과정은,

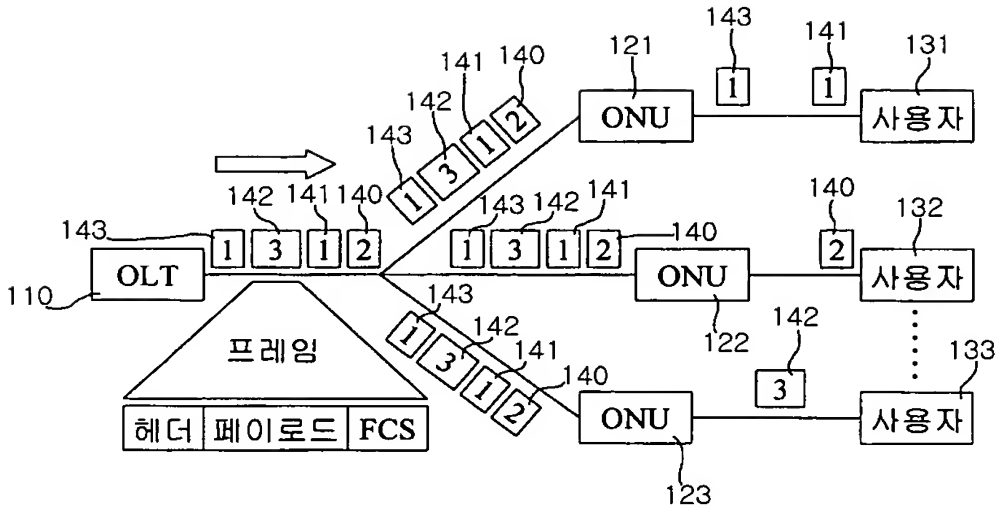
상기 광가입자장치가 상기 광종단장치로부터 주기적으로 발견 게이트 메시지는 수신하지만, 일반 게이트 메시지를 지속적으로 수신하지 못하면 세션키 오류가 발생한 것으로 판단하는 것을 특징으로 하는 광종단장치와 광가입자장치간 키 복구 방법.

【청구항 35】

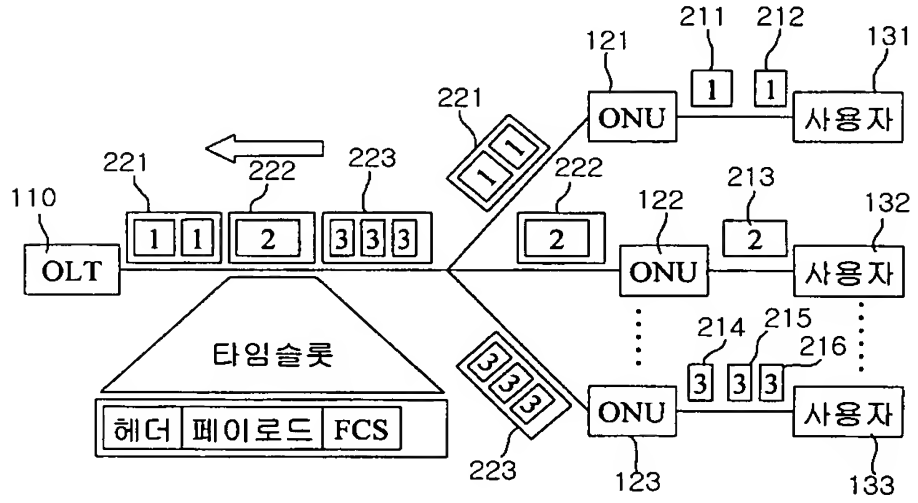
제 32항에 있어서, 상기 광가입자장치가 새로 생성한 세션키는 리포트 메시지에 실어져서 상기 광종단장치로 전송되는 것을 특징으로 하는 광종단장치와 광가입자장치간 키 복구 방법.

【도면】

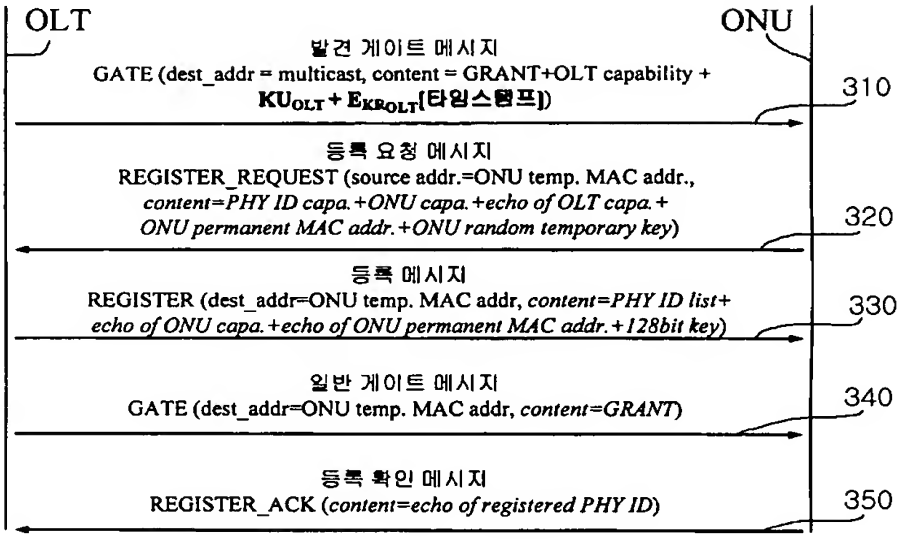
【도 1】


OLT
110
143
142
141
140
1
3
1
2
프레임
헤더
페이로드
FCS
ONU
121
122
123
131
132
133
사용자

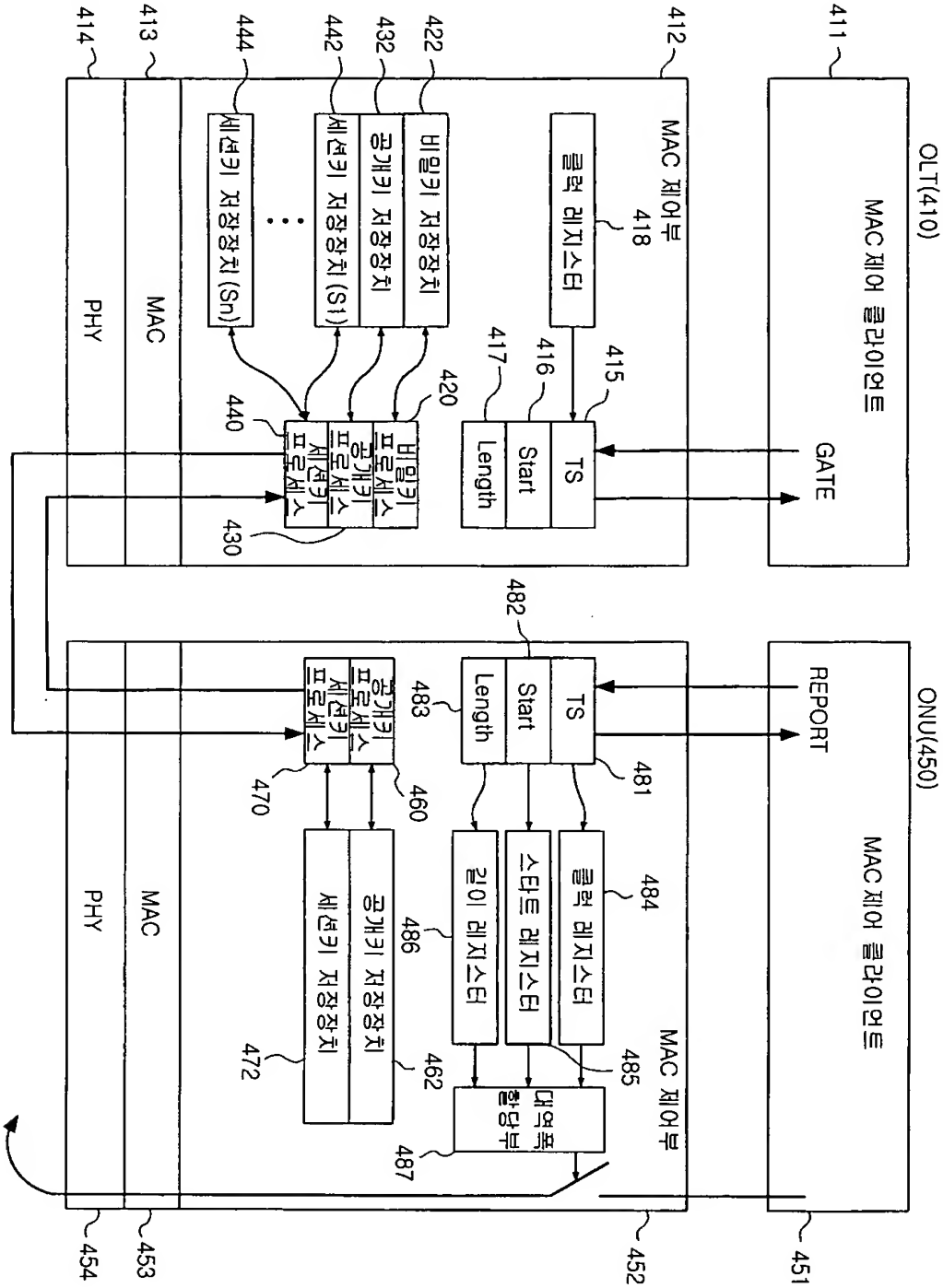
【도 2】


OLT
110
221
222
223
1
2
3
타임슬롯
헤더
페이로드
FCS
ONU
121
122
123
211
212
213
214
215
216
131
132
133
사용자

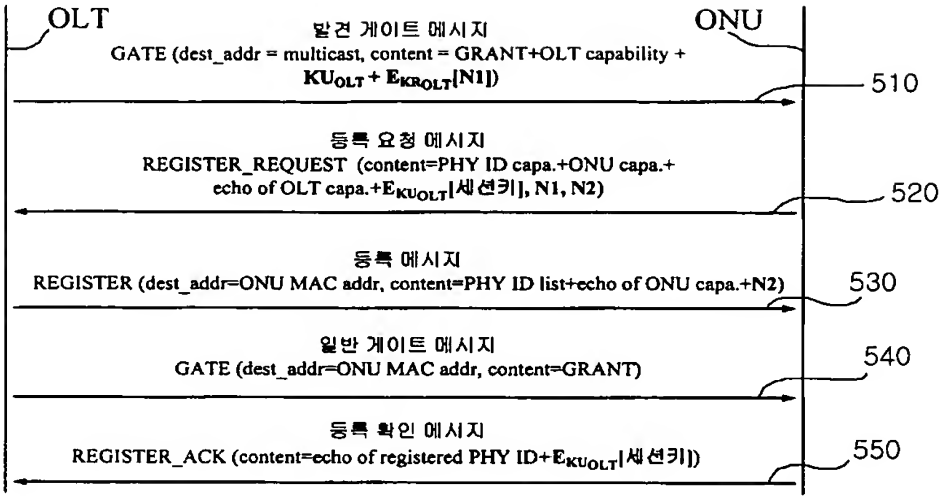
【도 3】


OLT
ONU
발견 게이트 메시지
GATE (dest_addr = multicast, content = GRANT+OLT capability +
KUOLT + EKROLT{타임스탬프})
310
등록 요청 메시지
REGISTER_REQUEST (source addr.=ONU temp. MAC addr.,
content=PHY ID capa.+ONU capa.+echo of OLT capa.+
ONU permanent MAC addr.+ONU random temporary key)
320
등록 메시지
REGISTER (dest_addr=ONU temp. MAC addr, content=PHY ID list+
echo of ONU capa.+echo of ONU permanent MAC addr.+128bit key)
330
일반 게이트 메시지
GATE (dest_addr=ONU temp. MAC addr, content=GRANT)
340
등록 확인 메시지
REGISTER_ACK (content=echo of registered PHY ID)
350

【도 4】


OLT(410)
MAC 제어 클라이언트
GATE
411
412
MAC 제어부
418
클럭 레지스터
416
417
415
TS
Start
Length
420
422
432
442
444
비밀키 저장장치
공개키 저장장치
세션키 저장장치 (S1)
세션키 저장장치 (Sn)
440
비밀키 프로세스
공개키 프로세스
세션키 프로세스
430
413
414
MAC
PHY
ONU(450)
MAC 제어 클라이언트
REPORT
482
TS
Start
Length
481
483
공개키 프로세스
세션키 프로세스
470
460
484
클럭 레지스터
486
길이 레지스터
스타트 레지스터
485
462
대역폭 할당부
487
472
공개키 저장장치
세션키 저장장치
MAC 제어부
452
451
453
454
MAC
PHY

【도 5】


OLT
ONU
발견 게이트 메시지
GATE (dest_addr = multicast, content = GRANT+OLT capability + KUOLT + EKROLT[N1])
510
등록 요청 메시지
REGISTER_REQUEST (content=PHY ID capa.+ONU capa.+ echo of OLT capa.+EKUOLT[세션키], N1, N2)
520
등록 메시지
REGISTER (dest_addr=ONU MAC addr, content=PHY ID list+echo of ONU capa.+N2)
530
일반 게이트 메시지
GATE (dest_addr=ONU MAC addr, content=GRANT)
540
등록 확인 메시지
REGISTER_ACK (content=echo of registered PHY ID+EKUOLT[세션키])
550